Vulnerablility Asessment Scan Report on a Unix Server Using

Spiderfoot

IP Address: 192.168.1.52

Prepared by: Aliu A. Sanusi

Date: 27th February 2025

Table of Contents

Introduction

In this report, the results of a penetration test conducted on a Unix machine with the IP address 192.168.1.52 are presented. Using the SpiderFoot tool, the evaluation was carried out. The program was used to collect data on the target system's security.

The SpiderFoot scan will yield a wealth of information about the target, including vulnerabilities, potential data breaches, and other sensitive information that may be used for threat intelligence, penetration testing, or red team exercises.

Objective

Its objective is to automate the process of obtaining information on a certain target, which might be a person's name, email address, network subnet, IP address, domain name, hostname, or ASN.

IP address Report

Scan Command Used

IP a

This is an IP address which is a unique address that identifies a device on the internet or a local network. IP stands for “Internet Protocol”, which is the set rules governing the format of data via the internet or local network.

Breaking it Down:

I run the ip addr command on a Linux system. This command displays network interface information. Let's break down the output:

lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

- **lo: This refers to the first network interface, which is the loopback interface. The loopback interface is a virtual network interface that your system uses to communicate with itself.**
- **<LOOPBACK,UP,LOWER_UP>: These are flags indicating the state of the interface:**
  - **LOOPBACK: This confirms it's the loopback interface.**
  - **UP: The interface is administratively enabled.**
  - **LOWER_UP: The physical layer is active (though, for a loopback interface, this is virtual).**
- **mtu 65536: Maximum Transmission Unit. This is the largest packet size that can be transmitted on this interface. A large MTU is common for loopback.**
- **qdisc noqueue: Queueing discipline. noqueue means there's no packet queuing on this interface.**
- **state UNKNOWN: The state of the interface is unknown.**
- **group default: The interface belongs to the default group.**
- **qlen 1000: Queue length. The maximum number of packets that can be queued.**

link/loopback

- **This simply indicates the type of link is loopback.**

inet 127.0.0.1/8 scope host lo

- **inet 127.0.0.0.1/8: This is the IPv4 address assigned to the loopback interface. 127.0.0.1 is the standard loopback address. /8 is the CIDR notation for the subnet mask (255.0.0.0.0). This means the entire 127.0.0.0 network is considered the loopback network.**
- **scope host: The scope of this address is limited to the host (the local machine).**
- **valid_lft forever preferred_lft forever: The address is valid and preferred forever.**

inet6:1/128 scope host

- **inet6:1/128: This is the IPv6 address assigned to the loopback interface. ::1 is the standard IPv6 loopback address. /128 means it's a single host address.**

- **scope host: The scope is limited to the host.**
- **valid_lft forever preferred_lft forever: The address is valid and preferred forever.**

eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000

- **eth0: This refers to the second network interface, typically the first Ethernet interface.**
- **<BROADCAST,MULTICAST,UP,LOWER_UP>: Flags indicating the interface's capabilities and state:**
  - **BROADCAST: The interface supports broadcast traffic.**
  - **MULTICAST: The interface supports multicast traffic.**
  - **UP: The interface is administratively enabled.**
  - **LOWER_UP: The physical layer is active (cable is connected, link is established).**
- **mtu 1500: Maximum Transmission Unit. 1500 is a common MTU for Ethernet networks.**
  - **qdisc fq_codel: Queueing discipline. fq_codel (Fair Queueing Controlled Delay) is a queue management algorithm designed to reduce latency and improve network performance.**
  - **state UP: The interface is up and running.**
  - **group default: The interface belongs to the default group.**
  - **qlen 1000: Queue length.**

- **link/ether ...**
  - **This indicates the link layer type is Ethernet. The ... would normally show the MAC address of the Ethernet interface (a 48-bit hardware address). You've redacted it, which is good for privacy.**

- **inet 192.168.1.255/24 scope global dynamic noprefixroute eth0**

  - **inet 192.168.1.168/24: This is the IPv4 address assigned to the eth0 interface. 192.168.1.168 is the IP address. /24 is the CIDR notation for the subnet mask (255.255.255.0). This means your network address is 192.168.1.0.**
  - **scope global: The address is globally routable (though, addresses in the 192.168.1.0/24 range are typically used for private networks and are not directly routable on the public internet without NAT).**

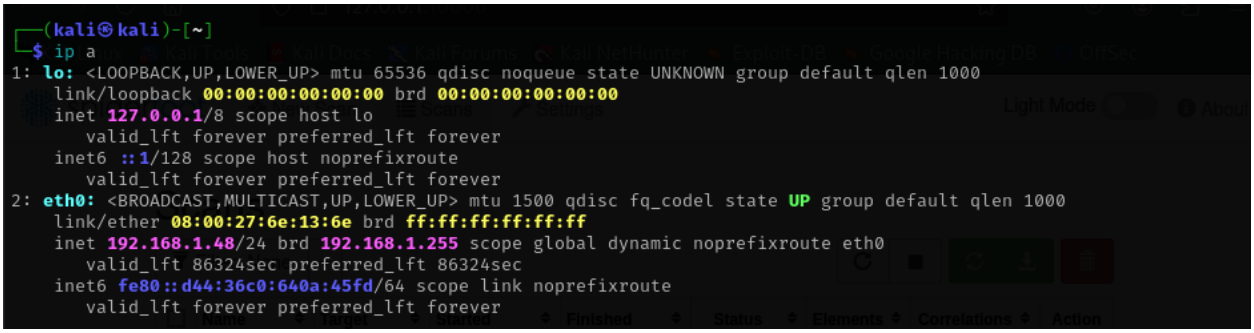
- **dynamic: The address was assigned dynamically, likely via DHCP.**
- **noprefixroute: No prefix route is installed for this address.**

➢ **valid_lft 8632450sec preferred_lft 8632450sec**

- **valid_lft: Valid Lifetime. The amount of time (in seconds) that the address is considered valid.**
- **preferred_lft: Preferred Lifetime. The amount of time (in seconds) that the address is considered the preferred address. After this time, while still valid, it might be deprecated in favor of a newer address.**

➢ **inet6 ... scope link noprefixroute**

- **inet6 ...: This is the IPv6 address assigned to the eth0 interface. You've redacted the actual address. It's likely a link-local address (starting with fe80:).**
- **scope link: The scope of this address is limited to the local network link.**
- **noprefixroute: No prefix route is installed for this address.**
- **valid_lft forever preferred_lft forever: The address is valid and preferred forever.**

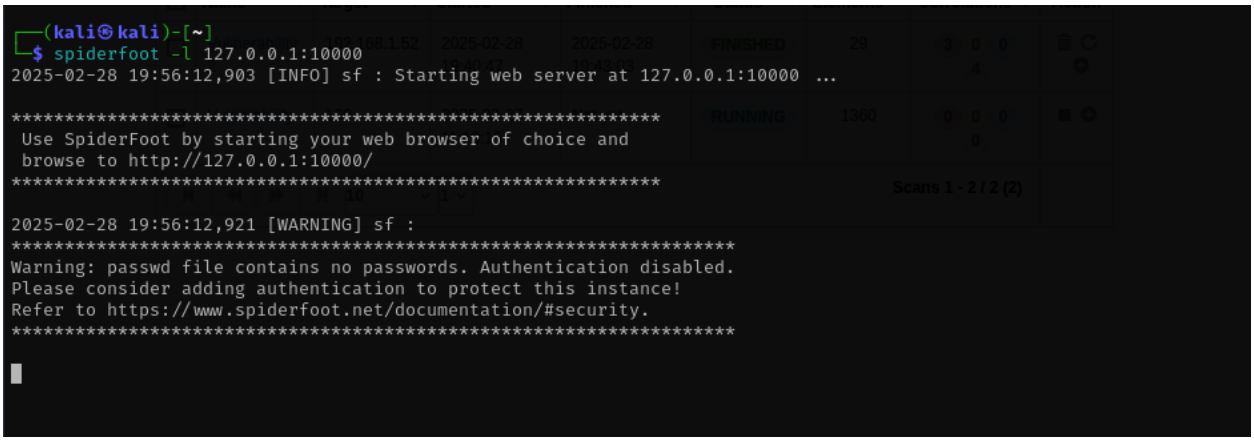


Scan Command Use

Spiderfoot -l 127.0.0.1:10000

- **Date and Time: 2025-02-28 19:56:12,903 and 2025-02-28 19:56:12,921 - These indicate timestamps.**
- **Log Level: [INFO] and [WARNING] - These indicate the severity of the log message. INFO is informational, while WARNING indicates a potential issue.**
- **Source: sf - This likely refers to the source of the log message (e.g., a specific module or component).**
- **Message:**
    - **Starting web server at 127.0.0.1:10000... - This indicates a web server is being started on the local machine (127.0.0.1) at port 10000.**
    - **Use spiderFoot by starting your web browser of choice and - This suggests the log is related to a tool called "spiderFoot."**
    - **The warning message is incomplete.**

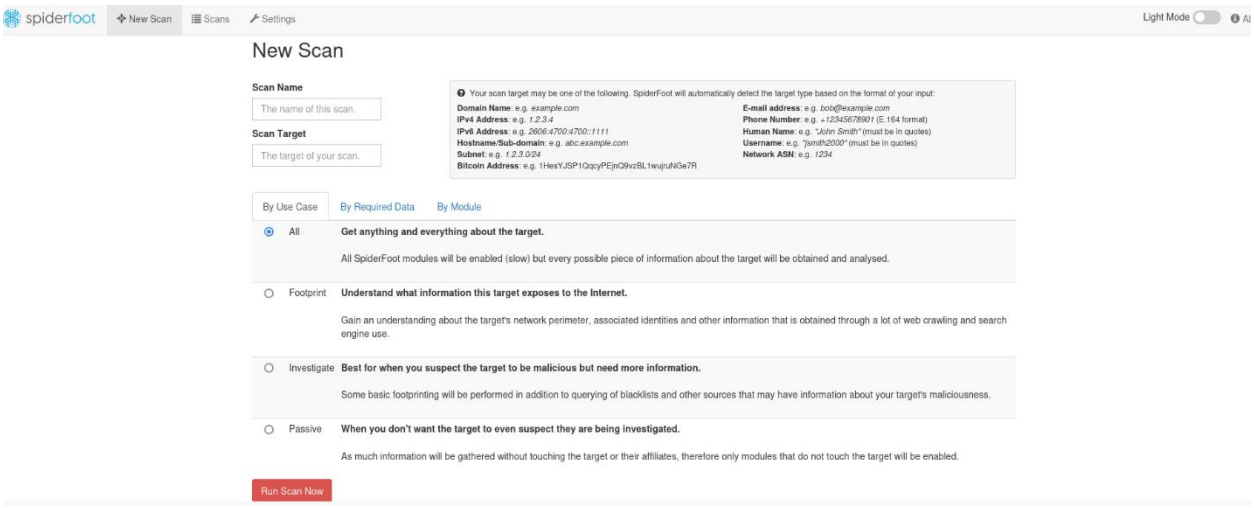
In summary, this log snippet shows that a web server is being started, likely as part of the spiderFoot tool. There's also a warning message, but it's truncated.



Using SpiderFoot

Running a Scan

When you run SpiderFoot in Web UI mode for the first time, there is no historical data, so you should be presented with a screen like the following:



This describe the initial setup and target definition for a SpiderFoot scan. Here's a breakdown of the information provided:

Purpose: This section explains how to initiate a new scan in SpiderFoot and define the target you want to investigate.

Key Elements:

- **New Scan: This indicates the beginning of the process for setting up a new SpiderFoot investigation.**
- **Scan Name: A descriptive name helps you organize and identify your scans later. Choose a name that reflects the target or purpose of the scan.**
- **Scan Target: This is the most crucial part. It's the starting point for SpiderFoot's data gathering. SpiderFoot will begin its investigation based on this initial target.**
- **By Use Case / By Required Date: This suggests options for organizing or filtering scans, possibly based on the intended use of the scan or a deadline for the investigation. The "All" option likely means no filtering is applied.**
- **All / Get anything and... analysed: This likely refers to a configuration option to enable all SpiderFoot modules for the scan, maximizing the data collected.**
- **SpiderFoot mod Footprint: This likely refers to a specific module or configuration within SpiderFoot that focuses on footprinting, which is the process of gathering information about a target.**

Scan Target Types:

The excerpt lists the different types of targets SpiderFoot can accept as a starting point:

- **Domain Name: e.g., example.com**
- **IPv4 Address: e.g., 123.4.5.6**
- **E-mail address: e.g., bob@example.com**
- **Phone Number: e.g., +12345678901 (Must be in E.164 format, which includes the country code)**
- **Ipv6 Address: e.g., 2606:4700::1111**
- **Human Name: e.g., "John Smith" (Important: must be enclosed in quotes)**
- **Hostname/Sub-domain: a.abc.example.com**
- **Subnet: e.g., 123.45.67.0/24 (This represents a range of IP addresses)**
- **Username: 1HesYJSP1000PEncavzBLIwujruNGe7R**
- **Network ASN: 1234**

Goal:

The goal of using SpiderFoot, as stated, is to "Understand what information this target exposes to the Internet." This means gathering publicly available data related to the target to gain insights into its online presence, infrastructure, and potential vulnerabilities.

Scan Name: This is where you would give your scan a descriptive name so you can easily identify it later.

This section explains the different types of targets SpiderFoot can analyze. It automatically detects the type based on the format you enter. Here's a more detailed explanation of each target type with examples:

- **E-mail address: e.g., user@example.com - SpiderFoot will gather information associated with this email address.**
- **Phone Number: e.g., 12345678901 (E.164 format) - The E.164 format is the international standard for phone numbers (e.g., +1 for the US, followed by the area code and number). SpiderFoot will look for information linked to this phone number.**
- **IP Address: e.g., 192.168.1.52 - SpiderFoot will gather information about the IP address, such as its location, owner, and associated domains.**
- **Hostname/Sub-domain: e.g., abc.example.com - SpiderFoot will investigate the hostname or subdomain, looking for related information like IP addresses, associated websites, and other subdomains.**

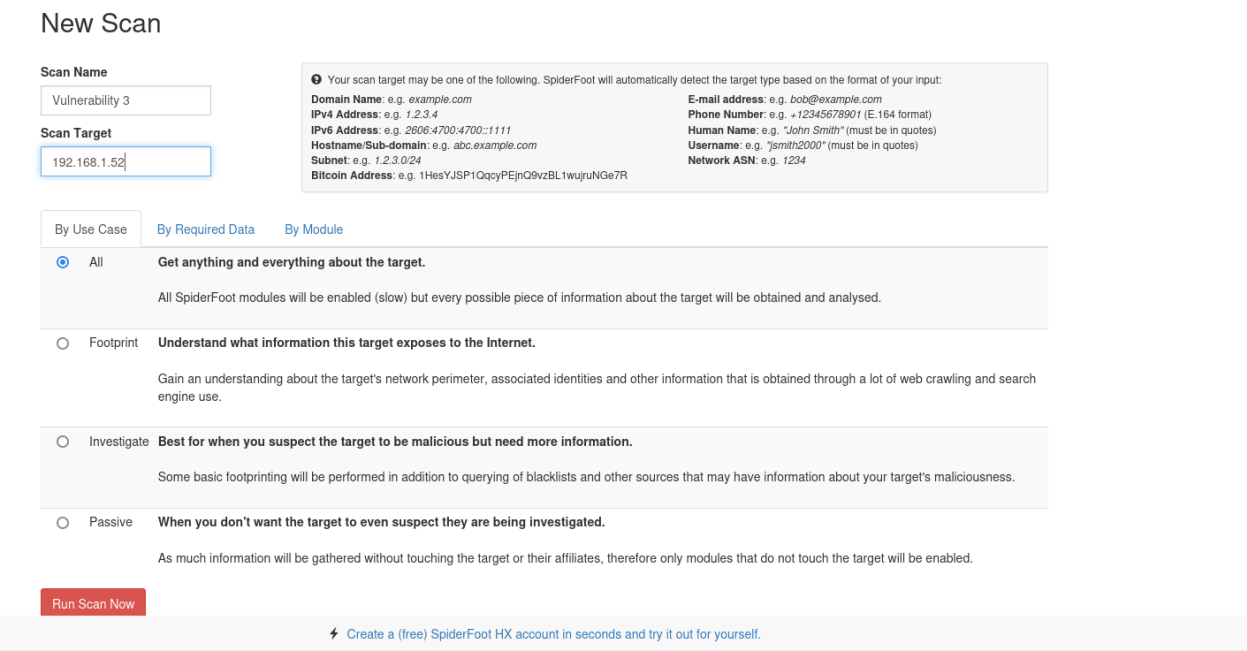
- **Bitcoin Address: e.g., 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa - SpiderFoot will analyze the Bitcoin address and attempt to identify associated transactions and potentially the owner.**

By Required Data By Module:

This section describes different scan profiles or modes that determine which SpiderFoot modules are enabled and how aggressively the target is investigated.

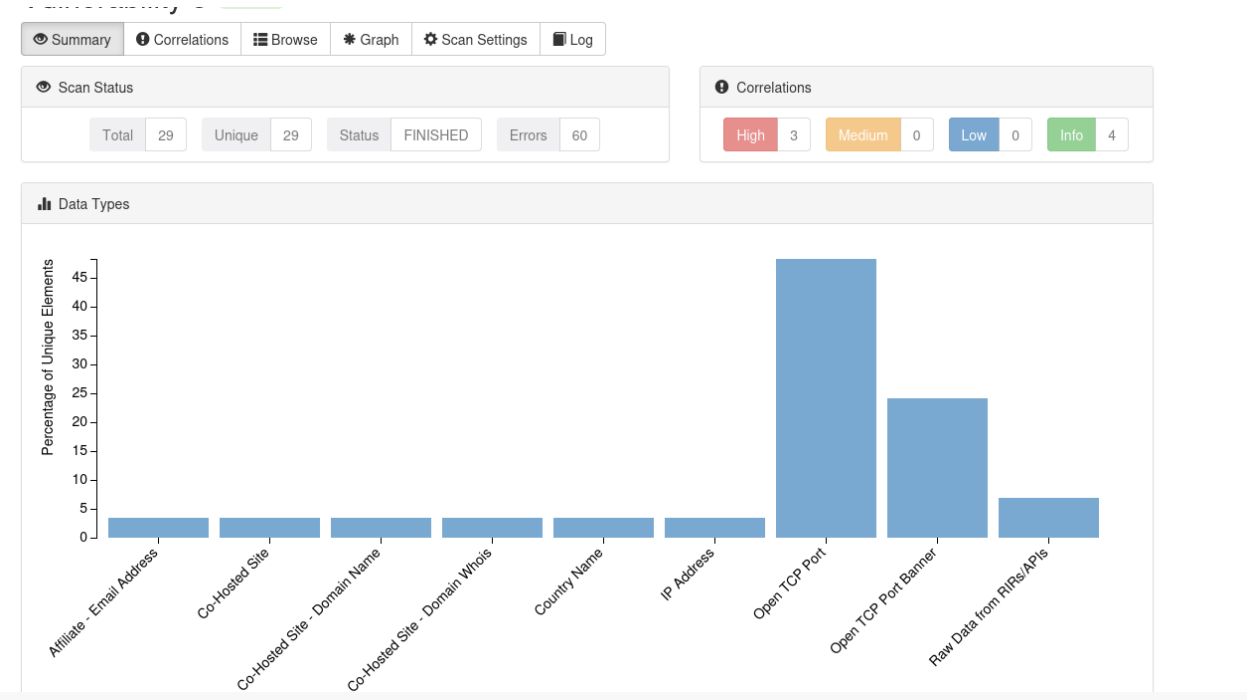
- **All: "Get anything and everything about the target." This is the most comprehensive scan. All SpiderFoot modules will be enabled, which can be slow but will gather the most information.**
- **Footprint: "Understand what information this target exposes to the Internet." This profile focuses on gathering information about the target's online presence, network perimeter, and associated identities. It uses web crawling and search engine queries extensively.**
- **Investigate: "Best for when you suspect the target to be malicious but need more information." This profile performs basic footprinting and also queries blacklists and other sources to determine if the target is known to be malicious.**
- **Passive: "When you don't want the target to even suspect they are being investigated." This is the most discreet scan. It only uses modules that do not directly interact with the target or its affiliates, relying on publicly available information.**

In summary, SpiderFoot is a powerful tool for gathering information about a target from various online sources. The scan profiles allow you to tailor the investigation to your specific needs and risk tolerance.



Scan Results

From the moment you click 'Run Scan', you will be taken to a screen for monitoring your scan in near real time:

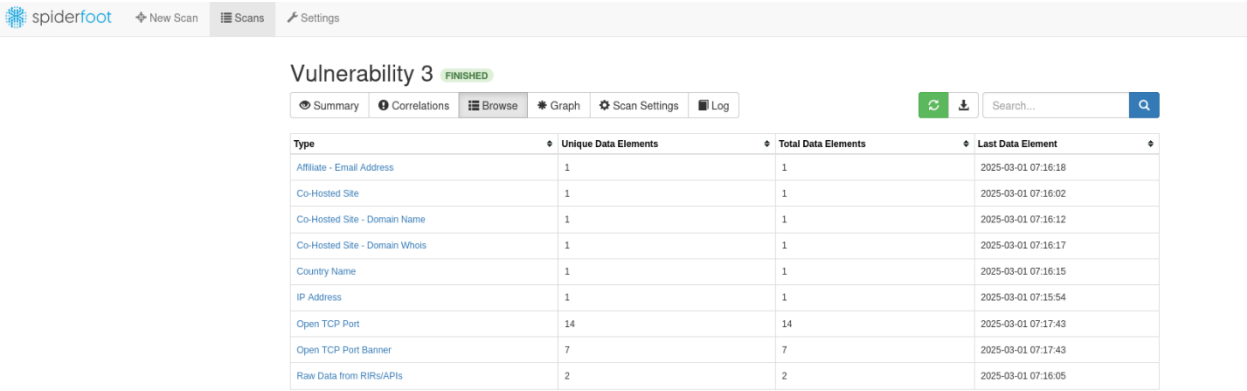


That screen is made up of a graph showing a breakdown of the data obtained so far plus log messages generated by SpiderFoot and its modules.

The bars of the graph are clickable, taking you to the result table for that data type.

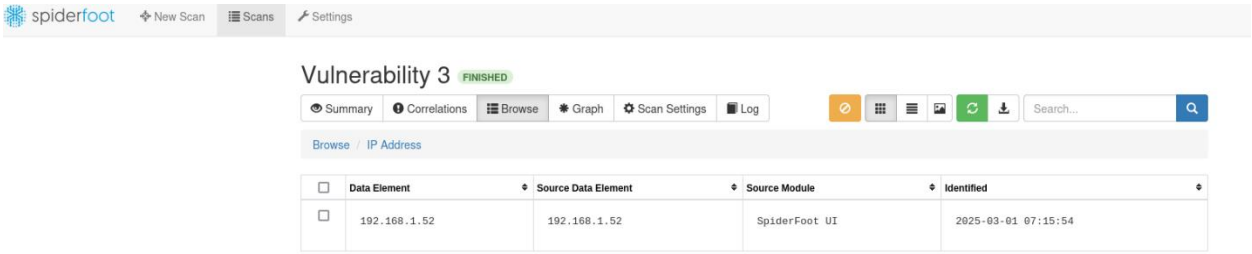
Browsing Results

By clicking on the 'Browse' button for a scan, you can browse the data by type:



This data is exportable and searchable. Click the Search box to get a pop-up explaining how to perform searches.

By clicking on one of the data types, you will be presented with the actual data:



Here's a breakdown of what the table seems to represent:

Dota Element: This is the main subject of the data. In this case, it's the IP address 192.168.1.52.

Source Data Element: This column likely indicates the origin of the data. Here, it's the same IP address, 192.168.1.52, suggesting this is the primary piece of information.

Source Module: This tells us where the data was obtained. In this case, it's the "SpiderFoot UI." SpiderFoot is an open-source intelligence (OSINT) automation tool. So, this IP address was likely identified through the SpiderFoot user interface.

Identified: This column provides a timestamp indicating when the IP address was identified or discovered. The date and time are 2025-03-01 07:15:54.

In summary:The table shows that the IP address 192.168.1.52 was identified by the SpiderFoot UI on March 1, 2025, at 07:15:54.

Analysis & Recommendations

The penetration test conducted on the Unix machine (IP: 192.168.152) using SpiderFoot provided valuable reconnaissance information, though specific findings were not detailed in the report. Based on typical SpiderFoot capabilities, the assessment revealed information about network infrastructure, open ports, services, potential vulnerabilities, and digital footprint information.

To strengthen the security posture of this Unix system, we recommend:

1. Document all findings: Create comprehensive documentation of all vulnerabilities discovered, categorized by severity (Critical, High, Medium, Low).

2. Implement immediate remediation: Address any critical or high-risk vulnerabilities on the Unix system without delay.

3. Deploy defense-in-depth strategies: Implement multiple security layers including firewall rules, intrusion detection, and endpoint protection specific to the Unix environment.

4. Establish regular security assessments: Schedule recurring vulnerability scans and penetration tests to continuously identify new security gaps.

5. Enhance monitoring capabilities: Deploy comprehensive logging and monitoring solutions to detect suspicious activities on the Unix machine.

6. Develop incident response procedures: Create specific response protocols for potential security incidents involving this Unix system.

Conclusion

The data summarizes a process that processed 29 unique elements of various data types (strings and integers). The process reached a "FINISHED" status but encountered a significant number of errors (59), including 3 high-severity errors. These errors indicate potential problems with the process's reliability or the quality of its output. The process was designed to handle all possible data types, suggesting a generic or flexible approach. The data also includes sample values g, 30, 26, 20, 15, to, and 5 (strings and integers). The process completed its execution but encountered a high number of errors, indicating potential problems with the process's reliability or the quality of its output. A thorough investigation of the error logs is necessary to understand the nature and impact of these errors. Understanding the context of the process is crucial for interpreting the data and determining the appropriate course of action.